DOI: https://doi.org/10.32782/PPSS.2023.1.15

ІНФОРМАЦІЯ ЯК КІБЕРЗБРОЯ У СУЧАСНОМУ СВІТІ

Алла Павлівна ГІРМАН,

канд. політ. наук, доцент кафедри міжнародних відносин факультету економіки, бізнесу та міжнародних відносин Університету митної справи та фінансів, м. Дніпро
https://orcid.org/0000-0003-0165-3700

INFORMATION AS A CYBER WEAPON IN TODAY'S WORLD

The rapid development of electronic technology and its growing integration into all spheres of life, including government and military administration, have led to a new kind of confrontation between states known as "information warfare." Specific means are being developed to conduct information warfare, which can be used both for defense and for attack. These can be controlled programs to destroy or distort information, block access to important data or disorganize the work of information resources, software viruses, intelligence programs, etc. Today, there are standard tools for detecting vulnerabilities in information systems. However, there is an urgent need to create a protection system with several levels, due to the possibility of interaction of all modern information systems through a single global communication network for users of any level.

Бурхливий розвиток електронної техніки та її зростаюча інтеграція у всі сфери життя, включаючи державне та військове управління, привели до нового виду протистояння між державами, відомого як "інформаційна війна". Інформаційна війна – це комплекс заходів, спрямованих на запобігання несанкціонованому використанню, пошкодженню чи знищенню елементів власної інформаційної інфраструктури, а також її використання з метою отримання інформаційної переваги у мирний час та під час підготовки та проведення військових операцій.

Для ведення інформаційної війни розробляються специфічні засоби, які можуть бути використані як для захисту, так і для нападу. Наступальні засоби програмно-технічного впливу включають в себе:

1. "Логічна бомба" – це прихована керуюча програма, яка може активуватися за певним сигналом або в заданий час з метою знищення або спотворення інформації, блокування доступу до важливих даних або дезорганізації роботи інформаційних ресурсів.

2. "Програмний вірус" – це спеціалізований програмний продукт, який може розповсюджувати "логічні бомби" і активувати їх у віддалених інформаційних мережах противника, автономно поширюватися та прикріплюватися до програм, а також передаватися по мережі.

3. "Троянський кінь" – це програма, яка дозволяє несанкціонований доступ до інформаційного ресурсу супротивника з метою збору розвідувальної інформації.

4. Нейтралізатор тестових програм, який забезпечує збереження дефектів програмного забезпечення.

5. Приховані інтерфейси для входу в систему, створені розробниками з корисливими або диверсійно-підривними цілями.

6. Малогабаритні пристрої, які здатні генерувати електромагнітні імпульси високої потужності для виведення з ладу радіоелектронної апаратури [1; 2].

Серед основних об'єктів застосування цих засобів можуть бути інформаційні елементи систем попередження про ракетний напад і контроль космічного простору, пункти управління вищої ланки та обчислювальні центри і вузли зв'язку. У мирний час такі засоби можуть використовуватися для атаки на банківську систему, систему управління повітряним рухом, системи управління гідроелектростанціями, а також для психологічного впливу на населення через засоби масової інформації.

Сьогодні існують стандартні інструменти для виявлення вразливих місць в інформаційних системах, і для забезпечення їх високого рівня захисту та цілісності важливо постійно слідкувати за системами, встановлювати оновлення та використовувати інструменти для відстоювання від можливих атак. Усі основні операційні системи, включаючи Microsoft Windows, Mac OS, GNU/Linux та OpenVMS, мають свої вразливості, і єдиним способом зменшення ризику їх використання – це постійний моніторинг і використання оновлених версій програмного забезпечення.

Необхідність створення системи захисту з декількома рівнями обумовлена можливістю взаємодії всіх сучасних інформаційних систем через єдину глобальну комунікаційну мережу для користувачів будь-якого рівня. Спеціалізовані засоби, такі як мережні шифратори та набір програмних технічних засобів, повинні гарантувати аутентифікацію користувачів, контроль доступу до інформаційних ресурсів, реєстрацію всіх дій споживачів та персоналу з можливістю оперативного та подальшого аналізу, а також забезпечити необхідний рівень конфіденційності.

Список використаних джерел:

1. Даник Ю. Г., Дупелич С. О. Стратегічні аспекти боротьби з робототехнічними комплексами. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2017. № 2(29). С. 16–25.

2. Хорошко В. О., Грищук Р. В. Кібернетична зброя: класифікація, базові принципи побудови, методи та засоби застосування й захисту від неї. *Сучасна спеціальна техніка*, 2016. №4. С.30-36.

3. Agarwal S. Secure Image Transmission Using Fractal and 2D-Chaotic Map // Journal of Imaging. 2018. Vol. 4 (1).

4. Castro D. (2018). Boosting the Cyberworkforce. URL: http://www.govtech.com/data/Boosting-the-Cyberworkforce.html

5. Get Involved with the CDM Learning Program! URL: https://www.uscert.gov/sites/default/files/cdm_files/FNR_CGB_MTG_AprilWebinar.pdf

6. Nasrullah, Sang J., Akbar M.A., Cai B., Xiang H., Hu H. Joint image compression and encryption using IWT with SPIHT, Kd-tree and chaotic maps. *Applied Sciences*. 2018. Vol. 8 (10).

7. National cybersecurity strategy of the USA. President D.J. Trump, Washington (September 2018). URL: https://d-russia.ru/wp-content/uploads/2019/01/National-Cyber-Strategy_USA_2018.pdf

8. Younas I., Khan M. A New Efficient Digital Image Encryption Based on Inverse Left Almost Semi Group and Lorenz Chaotic System. *Entropy*. 2018. Vol. 20 (12).